4765 PCIe Cryptographic Coprocessor Installation Manual

Note

Before using this information and the product it supports, read the information in “Safety and environmental notices” on page ix and in “Notices” on page 17.

First edition, May 2011

This edition describes installation of the IBM 4765 PCIe Cryptographic Coprocessor.

This and other publications related to the IBM 4765 PCIe Cryptographic Coprocessor can be obtained in PDF format from http://www.ibm.com/security/cryptocards.

Readers' comments can be communicated to IBM by using the product support link on the product Web site at http://www.ibm.com/security/cryptocards.

When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

© Copyright International Business Machines Corporation 2011.

US Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Figures v

Tables vii

Safety and environmental notices ix
Safety notices ix
World trade safety information x
Environmental notices xi
Product recycling and disposal xi
Battery return program xii
IBM cryptographic coprocessor card return program xiii

About this manual xv
How this manual is organized xv
Where to find more information xv

Chapter 1. Introduction 1
Contents of the coprocessor package 1
Special considerations for handling and storage 1
Storage 2
Temperature 2
Batteries 2
Requirements and specifications 2
Hardware requirement 2
Software requirement 2
Power requirements 2
Environmental specifications 2
Physical dimensions 3

Chapter 2. Installing the coprocessor 5

Chapter 3. Replacing coprocessor batteries 9

Chapter 4. Guidelines for transporting a coprocessor 13
Handling the coprocessor 13
International transport 13
Traveling with a coprocessor 13
Shipping a coprocessor 14

Notices 17
Trademarks 18
Electronic emissions 18
Federal Communications Commission (FCC) statement 18
Industry Canada Compliance Statement 18
Avis de conformité à la réglementation d'Industrie Canada 18
European Community Compliance Statement 18
Deutschsprachiger EU Hinweis: 19
VCCI Statement - Japan 20
IBM Taiwan Contact Information: 20
Electromagnetic Interference (EMI) Statement - Korea 20

Glossary 21

Index 23

Figures

1. Jumpers on the 4765 PCIe Cryptographic Coprocessor (front side) 6
2. IBM 4765 PCIe Cryptographic Coprocessor packaging material. 14

Tables

1. Operating, storage, and shipping environment specifications 3
2. Jumpers on the 4765 PCIe Cryptographic Coprocessor 7
3. Part numbers for batteries 9

Safety and environmental notices

Safety notices

Safety notices may be printed throughout this guide. **DANGER** notices warn you of conditions or procedures that can result in death or severe personal injury. **CAUTION** notices warn you of conditions or procedures that can cause personal injury that is neither lethal nor extremely hazardous. **Attention** notices warn you of conditions or procedures that can cause damage to machines, equipment, or programs. The following **DANGER** notices appear in this manual:

DANGER

When working on or around the system, observe the following precautions:

Electrical voltage and current from power, telephone, and communication cables are hazardous. To avoid a shock hazard:

- **Connect power to this unit only with the IBM® provided power cord. Do not use the IBM provided power cord for any other product.**
- **Do not open or service any power supply assembly.**
- **Do not connect or disconnect any cables or perform installation, maintenance, or reconfiguration of this product during an electrical storm.**
- **The product might be equipped with multiple power cords. To remove all hazardous voltages, disconnect all power cords.**
- **Connect all power cords to a properly wired and grounded electrical outlet. Ensure that the outlet supplies proper voltage and phase rotation according to the system rating plate.**
- **Connect any equipment that will be attached to this product to properly wired outlets.**
- **When possible, use one hand only to connect or disconnect signal cables.**
- **Never turn on any equipment when there is evidence of fire, water, or structural damage.**
- **Disconnect the attached power cords, telecommunications systems, networks, and modems before you open the device covers, unless instructed otherwise in the installation and configuration procedures.**
- **Connect and disconnect cables as described in the following procedures when installing, moving, or opening covers on this product or attached devices.**

  To disconnect:
  1. **Turn off everything (unless instructed otherwise).**
  2. **Remove the power cords from the outlets.**
  3. **Remove the signal cables from the connectors.**
  4. **Remove all cables from the devices.**

  To connect:
  1. **Turn off everything (unless instructed otherwise).**
  2. **Attach all cables to the devices.**
  3. **Attach the signal cables to the connectors.**
  4. **Attach the power cords to the outlets.**
  5. **Turn on the devices.**
- **Sharp edges, corners and joints may be present in and around the system. Use care when handling equipment to avoid cuts, scrapes and pinching.**

(D005)

The following **CAUTION** notices appear in this manual:

CAUTION:
Only trained service personnel may replace this battery. The battery contains lithium. To avoid possible explosion, do not burn or charge the battery.

Do Not:

- **Throw or immerse into water**
- **Heat to more than 100°C (212°F)**
- **Repair or disassemble**

Exchange only with the IBM-approved part. Recycle or discard the battery as instructed by local regulations. In the United States, IBM has a process for the collection of this battery. For information, call 1-800-426-4333. Have the IBM part number for the battery unit available when you call. (C002)

World trade safety information

Several countries require the safety information contained in product publications to be presented in their national languages. If this requirement applies to your country, a safety information booklet is included in the publication package shipped with the product. The booklet contains the safety information in your national language with references to the US English source. Before using a US English publication to install, operate, or service this IBM product, you must first become familiar with the related safety information in the booklet. You should also refer to the booklet any time you do not clearly understand any safety information in the US English publications.

Environmental notices

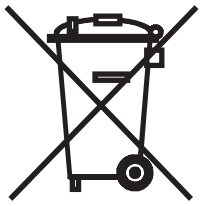
Product recycling and disposal

This unit must be recycled or discarded according to applicable local and national regulations. IBM encourages owners of information technology (IT) equipment to responsibly recycle their equipment when it is no longer needed. IBM offers a variety of product return programs and services in several countries to assist equipment owners in recycling their IT products. Information on IBM product recycling offerings can be found on IBM's Internet site at:

http://www.ibm.com/ibm/environment/products

Esta unidad debe reciclarse o desecharse de acuerdo con lo establecido en la normativa nacional o local aplicable. IBM a los propietarios de equipos de tecnología de la información (TI) que reciclen responsablemente sus equipos cuando éstrecomiendaos ya no les sean útiles. IBM dispone de una serie de programas y servicios de devolución de productos en varios países, a fin de ayudar a los propietarios de equipos a reciclar sus productos de TI. Se puede encontrar información sobre las ofertas de reciclado de productos de IBM en el sitio web de IBM:

http://www.ibm.com/ibm/environment/products



Notice: This mark applies only to countries within the European Union (EU) and Norway.

Appliances are labeled in accordance with European Directive 2002/96/EC concerning waste electrical and electronic equipment (WEEE). The Directive determines the framework for the return and recycling of used appliances as applicable throughout the European Union. This label is applied to various products to indicate that the product is not to be thrown away, but rather reclaimed upon end of life per this Directive.

In accordance with the European WEEE Directive, electrical and electronic equipment (EEE) is to be collected separately and to be reused, recycled, or recovered at end of life. Users of EEE with the WEEE marking per Annex IV of the WEEE Directive, as shown above, must not dispose of end of life EEE as unsorted municipal waste, but use the collection framework available to customers for the return, recycling, and recovery of WEEE. Customer participation is important to minimize any potential effects of EEE on the environment and human health due to the potential presence of hazardous substances in EEE. For proper collection and treatment, contact your local IBM representative.

For the European Union:

注意: このマークは EU 諸国およびノルウェーにおいてのみ適用されます。

この機器には、EU 諸国に対する廃電気電子機器指令 2002/96/EC(WEEE) のラベルが貼られています。この指令は、EU 諸国に適用する使用済み機器の回収とリサイクルの骨子を定めています。このラベルは、使用済みになった時に指令に従って適正な処理をする必要があることを知らせるために種々の製品に貼られています。

Remarque : Cette marque s'applique uniquement aux pays de l'Union Européenne et à la Norvège.

L'étiquette du système respecte la Directive européenne 2002/96/EC en matière de Déchets des Equipements Electriques et Electroniques (DEEE), qui détermine les dispositions de retour et de recyclage applicables aux systèmes utilisés à travers l'Union européenne. Conformément à la directive, ladite étiquette précise que le produit sur lequel elle est apposée ne doit pas être jeté mais être récupéré en fin de vie.

Battery return program

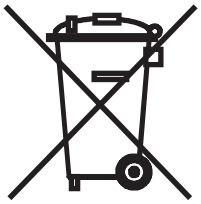
This product contains lithium batteries. Consult your user manual or service manual for specific battery information. The batteries must be recycled or disposed of properly. Recycling facilities may not be available in your area. For information on disposal of batteries outside the United States, go to *http://www.ibm.com/ibm/environment/products/index.shtml* or contact your local waste disposal facility.

In the United States, IBM has established a return process for reuse, recycling, or proper disposal of used IBM sealed lead acid, nickel cadmium, nickel metal hydride, and other battery packs from IBM Equipment. For information on proper disposal of these batteries, contact IBM at 1-800-426-4333.

In Taiwan, the following applies:

Please recycle batteries

廢電池請回收



Notice: This mark applies only to countries within the European Union (EU) and Norway.

Batteries or packaging for batteries are labeled in accordance with European Directive 2006/66/EC concerning batteries and accumulators and waste batteries and accumulators. The Directive determines the framework for the return and recycling of used batteries and accumulators as applicable throughout the European Union. This label is applied to various batteries to indicate that the battery is not to be thrown away, but rather reclaimed upon end of life per this Directive.

バッテリーあるいはバッテリー用のパッケージには、EU 諸国に対する廃電気電子機器指令 2006/66/EC のラベルが貼られています。この指令は、バッテリーと蓄電池、および廃棄バッテリーと蓄電池に関するものです。この指令は、使用済みバッテリーと蓄電池の回収とリサイクルの骨子を定めているもので、EU 諸国にわたって適用されます。このラベルは、使用済みになったときに指令に従って適正な処理をする必要があることを知らせるために種々のバッテリーに貼られています。

Les batteries ou emballages pour batteries sont étiquetés conformément aux directives européennes 2006/66/EC, norme relative aux batteries et accumulateurs en usage et aux batteries et accumulateurs usés. Les directives déterminent la marche à suivre en vigueur dans l'Union Européenne pour le retour et le recyclage des batteries et accumulateurs usés. Cette étiquette est appliquée sur diverses batteries pour indiquer que la batterie ne doit pas être mise au rebut mais plutôt récupérée en fin de cycle de vie selon cette norme.

In accordance with the European Directive 2006/66/EC, batteries and accumulators are labeled to indicate that they are to be collected separately and recycled at end of life. The label on the battery may also include a chemical symbol for the metal concerned in the battery (Pb for lead, Hg for mercury and Cd for cadmium). Users of batteries and accumulators must not dispose of batteries and accumulators as unsorted municipal waste, but use the collection framework available to customers for the return, recycling and treatment of batteries and accumulators. Customer participation is important to minimize any potential effects of batteries and accumulators on the environment and human health due to the potential presence of hazardous substances. For proper collection and treatment, contact your local IBM representative.

For California:

Perchlorate Material - special handling may apply.

See http://www.dtsc.ca.gov/hazardouswaste/perchlorate.

The foregoing notice is provided in accordance with California Code of Regulations Title 22, Division 4.5 Chapter 33. Best Management Practices for Perchlorate Materials. This product, part or both may include a lithium manganese dioxide battery which contains a perchlorate substance

IBM cryptographic coprocessor card return program

The cryptographic coprocessor card includes a polyurethane material that contains mercury. Please follow Local Ordinances or regulations for disposal of this card. IBM has established a return program for certain IBM cryptographic coprocessor cards. More information can be found at: *http://www.ibm.com/ibm/environment/products/prp.shtml*

برنامج ارجاع كرت IBM Cryptographic Coprocessor

هـذه الماكيـنة قد تحتـوي على خاصـية اختيارية، وهى كـارت
Cryptographic Coprocessor
والتي تحتـوي على مـادة بولـييوريثيـن التي تحتـوي على الزئبـق
رجـاء اتبـاع القوانيـن أو التعليمـات المحـلية للتخـلص من هـذا الكـارت .
قامـت شركة IBM باعداد برنامج لارجاع بعض كـروت IBM Cryptographic
Coprocessor

لمزيد من المعلومات، رجاء زيارة الموقع
http://www.ibm.com/ibm/environment/products/prp.shtml

About this manual

This manual is written for personnel installing the IBM 4765 PCIe Cryptographic Coprocessor hardware.

How this manual is organized

This manual is organized as follows:

- "Safety and environmental notices" on page ix describes important general safety and environmental information.
- Chapter 1, "Introduction," describes the contents of the coprocessor packages; shipping, handling, and storage considerations; and requirements and specifications of the PCIe cryptographic coprocessor.
- Chapter 2, "Installing the coprocessor," describes the procedure to physically install the PCIe cryptographic coprocessor.
- Chapter 3, "Replacing coprocessor batteries," describes the way to replace the batteries on the PCIe cryptographic coprocessor.
- Chapter 4, "Guidelines for transporting a coprocessor," on page 13 provides guidance for shipping or traveling with the PCIe cryptographic coprocessor.
- Notices contains notices for various countries, trademark information, and information about the product warranty extended by IBM.

A glossary and an index complete the manual.

Where to find more information

Visit the IBM product Web site at http://www.ibm.com/security/cryptocards to obtain IBM 4765-related publications. This and other publications are available as Adobe PDF files that you can read and print with the Adobe Acrobat Reader.

Before installing a coprocessor, check the IBM ServerProven® list on the IBM product Web site, http://www.ibm.com/security/cryptocards, for the approved server list.

Chapter 1. Introduction

This section details the contents of the IBM 4765 PCIe Cryptographic Coprocessor package and describes the following information:

- Special considerations for handling and storage
- Requirements and specifications

The cryptographic the coprocessor uses dedicated hardware to process cryptographic keys, certificates, and bulk data. These cryptographic functions are performed within a tamper-resistant module that is validated to the Federal Information Processing Standard (FIPS) PUB 140-2 Level 4, as established by the National Institute of Standards and Technology. This is a standard of detecting and responding to unauthorized attempts at physical access and security compromise due to environmental conditions such as voltage and temperature.

You can install the coprocessor, a standard height, half-length PCIe adapter card, only in an IBM System x® x86 approved server with at least two, possibly three adjacent PCIe expansion slots available.

Before installing a coprocessor, check the IBM product Web site, http://www.ibm.com/security/cryptocards, for the IBM ServerProven list.

Contents of the coprocessor package

Your coprocessor package includes the following items:

- The IBM 4765 PCIe Cryptographic Coprocessor
- *IBM License Agreement for Machine Code*, SC28-6872-01 (multi-language)
- *IBM License Agreement for Machine Code Addendum for Elliptical Curve Cryptography*, GC27-2612-00 (multi-language)
- *IBM 4765 PCIe Cryptographic Coprocessor Safety Notices*, G325-2638-00
- *IBM 4765 PCIe Cryptographic Coprocessor Statement of Limited Warranty - Warranty Information flyer*, SC23-6884-00
- Notice to Users of the IBM 4765 PCIe Cryptographic Coprocessor, PN 80Y2344
- Slot cover label instructions with two self-adhesive warning labels for adjacent expansion slot covers, PN 46K3930

If any item is missing or damaged, contact your local IBM representative.

Special considerations for handling and storage

Each coprocessor is shipped from the factory with a certified device key. This electronic key, which is stored in the card's battery-backed protected memory, digitally signs test messages to confirm that the coprocessor is genuine and that no tampering has occurred.

Note: If any of the secure module’s tamper sensors is triggered by tampering or accident, the coprocessor erases (zeroizes) all data in the protected memory, destroying the device key. This renders the coprocessor permanently inoperable, and there is no recovery from this situation.

The coprocessor cannot operate without the device key. To protect the key, follow these temperature and battery guidelines:

Storage

It is recommended that an uninstalled coprocessor be kept in its original protective packaging material. Save this packaging material for future use, especially if the coprocessor must be transported to another location.

Temperature

Do not expose the coprocessor to temperatures outside the limits in Table 1 on page 3.

Batteries

Do not remove battery power from the coprocessor. Data in the protected memory is lost (zeroized) when battery power is removed, rendering the coprocessor permanently inoperable. For information about replacing the batteries without erasing the protected memory, see Chapter 3, “Replacing coprocessor batteries.”

Requirements and specifications

Hardware requirement

The coprocessor must be installed in an IBM System x x86 approved server from the IBM ServerProven list with at least two, possibly three PCIe (Version 1.1) bus slots available that are adjacent. See notes below. No additional hardware or cabling is required.

Notes:

1. The USB port mini AB connector is for development use only. It is not intended for customer use.
2. The two RJ45 connectors are blocked. They are not intended for customer use.
3. For thermal/cooling reasons, an IBM 4765 PCIe Cryptographic Coprocessor must not have any other adapter of any type installed in a slot adjacent to it. Installing an adapter adjacent to the IBM 4765 PCIe Cryptographic Coprocessor invalidates the product warranty.
4. An IBM 4765 PCIe Cryptographic Coprocessor can be installed in an end slot, which requires a total of two slots that are adjacent. Otherwise, a total of three slots that are adjacent is required.

Software requirement

- The coprocessor requires support software, for example, the IBM 4765 CCA Support Program, for both the host machine and for its internal firmware. Operating system support is determined by the support software.

  This publication does not discuss the installation of support software. For information about the latest software features available, visit the product Web site at http://www.ibm.com/security/cryptocards.

Power requirements

The power requirements for the IBM 4765 PCIe Cryptographic Coprocessor are:

- +12 volt PCIe domain: 20.13 watts maximum
- +3.3 volt PCIe domain: 3.31 watts maximum (including USB external load)
- On-board batteries: batteries dead less than 2.4 volts; low-battery warning less than 2.75 volts

Environmental specifications

The environmental specifications for the IBM 4765 PCIe Cryptographic Coprocessor are shown in Table 1 on page 3.

Table 1. Operating, storage, and shipping environment specifications

	Operating environment	**Storage environment**	**Shipping environment**
Temperature	+10°C - +35°C (+50°F - +95°F)	+1°C - +60°C (+33.8°F - +140°F)	-34°C - +60°C (-29.2°F - +140°F)
Relative humidity	8 - 80%	5 - 80%	5 - 100%
Wet bulb	< +27.0°C (+80.6°F)	< +29.0°C (+84.2°F)	< +29.0°C (+84.2°F)
Pressure (minimum)	700 mbar (maximum altitude 10 000 feet)	700 mbar	550 mbar

Physical dimensions

- The coprocessor is a standard height, half-length PCIe adapter card
- 4.376 inches by 6.6 inches (111.15 mm by 167.65 mm).

Chapter 2. Installing the coprocessor

This section describes installing the IBM 4765 PCIe Cryptographic Coprocessor.

Note: It is not necessary to install the support software before installing a coprocessor.

To install the coprocessor into the host computer, follow these steps:

1. Locate your computer's instructions for installing expansion cards. Throughout this procedure, follow the safety instructions in that manual.
2. Turn OFF the computer and all attached devices.
3. Disconnect all cables, including the power cable.

DANGER

When working on or around the system, observe the following precautions:

Electrical voltage and current from power, telephone, and communication cables are hazardous. To avoid a shock hazard:

- **Connect power to this unit only with the IBM provided power cord. Do not use the IBM provided power cord for any other product.**
- **Do not open or service any power supply assembly.**
- **Do not connect or disconnect any cables or perform installation, maintenance, or reconfiguration of this product during an electrical storm.**
- **The product might be equipped with multiple power cords. To remove all hazardous voltages, disconnect all power cords.**
- **Connect all power cords to a properly wired and grounded electrical outlet. Ensure that the outlet supplies proper voltage and phase rotation according to the system rating plate.**
- **Connect any equipment that will be attached to this product to properly wired outlets.**
- **When possible, use one hand only to connect or disconnect signal cables.**
- **Never turn on any equipment when there is evidence of fire, water, or structural damage.**
- **Disconnect the attached power cords, telecommunications systems, networks, and modems before you open the device covers, unless instructed otherwise in the installation and configuration procedures.**
- **Connect and disconnect cables as described in the following procedures when installing, moving, or opening covers on this product or attached devices.**

  To disconnect:
  a. Turn off everything (unless instructed otherwise).
  b. Remove the power cords from the outlets.
  c. Remove the signal cables from the connectors.
  d. Remove all cables from the devices.

  To connect:
  a. Turn off everything (unless instructed otherwise).
  b. Attach all cables to the devices.
  c. Attach the signal cables to the connectors.
  d. Attach the power cords to the outlets.
  e. Turn on the devices.
- **Sharp edges, corners and joints may be present in and around the system. Use care when handling equipment to avoid cuts, scrapes and pinching.**

(D005)

4. Choose a PCIe expansion slot able to accommodate a standard short-type adapter card. Any adjacent slots must be empty.

For thermal/cooling reasons, any slots that are adjacent to the PCIe expansion slot ***must be empty*** to allow for adequate airflow. It is permissible to install an IBM 4765 PCIe Cryptographic Coprocessor in an end slot. Place a warning label on the expansion slot cover of each adjacent slot that reads: "Leave this slot empty while IBM 4765 is in adjacent slot."

Note: Installing any adapter adjacent to an IBM 4765 invalidates the product warranty.

5. If the expansion slot has an individual cover, remove any bracket-holding screw and the cover.

   Attention: Electrostatic discharge (ESD) can damage the card and its components. Wear an ESD wrist-strap while handling and installing the card, or take the following precautions:

   - Limit your movements; this helps prevent static electricity from building up around you.
   - Prevent others from touching the card or other components.
   - Before removing the card from the electrostatic discharge (ESD) barrier bag, touch the bag to an unpainted metal surface on your computer and hold it there for at least two seconds.

   Handle the card by its edges only. Do not touch exposed circuitry and components.
6. Remove the cryptographic coprocessor from its ESD barrier bag. Do not discard the bag. It can be used again whenever the coprocessor is removed from the server.
7. Verify that the jumpers on the card are positioned correctly; see Figure 1 and Table 2 on page 7.

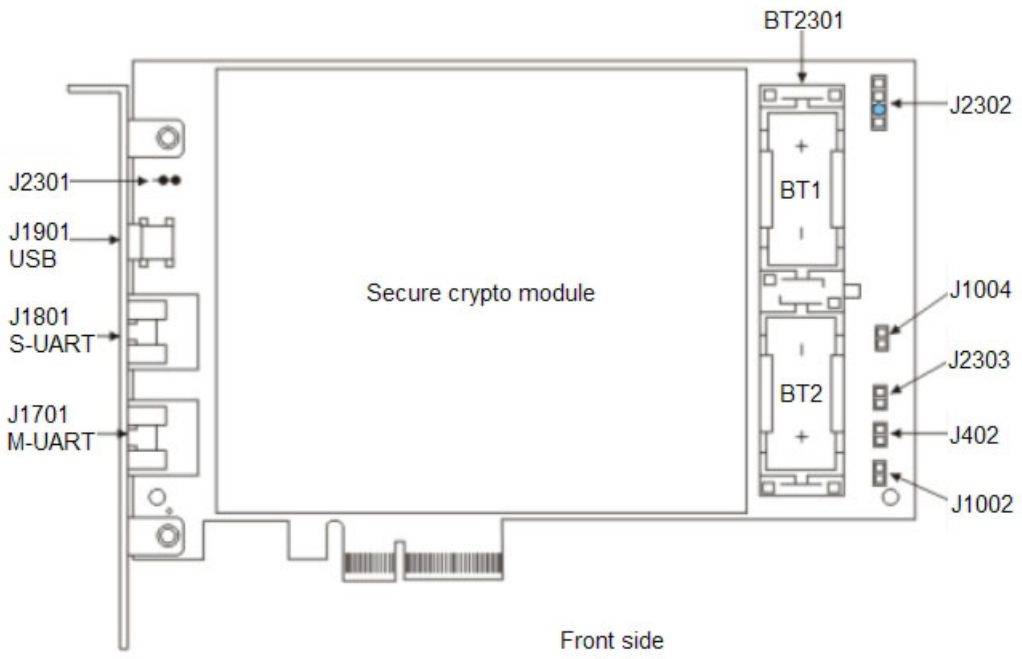


Figure 1. Jumpers on the 4765 PCIe Cryptographic Coprocessor (front side)

Table 2. Jumpers on the 4765 PCIe Cryptographic Coprocessor

Jumper	Number of pins	Name of jumper	Position when shipped
J402	2	External intrusion latch connect	Shipped without jumper installed (do not connect card circuit to host circuit for warning activation)
J1002	2	VPD EEPROM write	Shipped with Berg jumper installed (flash write enabled)
J1004	2	Base FPGA PERST re-program	Shipped with Berg jumper installed (allow reprogramming)
J2301	2	Battery disconnect wire	Shipped with jumper (wire loop) installed (cut wire to zeroize card)
J2302	3 (keyed)	Temporary-battery connector	Shipped without jumper installed (used to plug in battery-replacement tray)
J2303	2	External intrusion latch disable	Shipped with Berg jumper installed (disable warning activation)

Note: *Shipped with jumper installed* means that the pins are connected.

8. Insert the coprocessor into the slot; be sure that the card is fully seated.

   For thermal/cooling reasons, be sure that no other adapter of any type is installed in any slot adjacent to the coprocessor. Installing an adapter adjacent to the coprocessor invalidates the product warranty.
9. If possible, install a bracket-holding screw. Some server models have a row of screws available inside the machine for this purpose.
10. Replace the host computer's cover.
11. Reconnect the power cable and any other cables you disconnected.
12. Turn the computer ON. The cryptographic coprocessor runs its power-on self-test (POST).

You have completed the procedure for the physical installation of the PCIe cryptographic coprocessor. Refer to the support software documentation for information about initializing and using the coprocessor.

Chapter 3. Replacing coprocessor batteries

This section describes the way to replace the batteries on the IBM 4765 PCIe Cryptographic Coprocessor.

Two lithium batteries mounted on the IBM 4765 PCIe Cryptographic Coprocessor supply power to the card's components, including protected memory. Your support software or application software can query the coprocessor to determine whether the batteries need to be replaced.

When shipped from the factory, the protected memory contains a certified device key. If your coprocessor has been initialized by support software, the protected memory contains secret data, including a master cryptographic key, user profiles, and user passwords.

Attention: If you remove either of the batteries without first backing up the power with a fresh battery, the data in protected memory can be lost. This renders the coprocessor permanently inoperable. The battery-replacement kit for the IBM 4765 PCIe Cryptographic Coprocessor provides the battery tray needed to provide backup power while you replace the batteries. The kit also includes two replacement batteries. A multi-battery replacement pack, containing 20 replacement batteries, is available for users who have a battery tray. See Table 3.

Table 3. Part numbers for batteries

P/N	Description	Contents
45D5803	Battery-replacement kit	• Two replacement batteries • One battery tray with connecting wires • Two battery-attention labels
74Y0465	Multi-battery replacement pack	• Twenty replacement batteries • Twenty battery-attention labels • Requires one battery tray for installing batteries

To order the kit or the pack, contact your local IBM System z® representative.

CAUTION:
Only trained service personnel may replace this battery. The battery contains lithium. To avoid possible explosion, do not burn or charge the battery.

Do Not:

- **Throw or immerse into water**
- **Heat to more than 100°C (212°F)**
- **Repair or disassemble**

Exchange only with the IBM-approved part. Recycle or discard the battery as instructed by local regulations. In the United States, IBM has a process for the collection of this battery. For information, call 1-800-426-4333. Have the IBM part number for the battery unit available when you call. (C002)

To replace the on-board batteries, follow these steps:

1. Have on hand two good replacement batteries, one battery tray, and two battery attention labels. See Table 3. Verify that the batteries are good.
2. Turn OFF the computer and all attached devices.
3. Disconnect all cables, including any power cables.

DANGER

When working on or around the system, observe the following precautions:

Electrical voltage and current from power, telephone, and communication cables are hazardous. To avoid a shock hazard:

- **Connect power to this unit only with the IBM provided power cord. Do not use the IBM provided power cord for any other product.**
- **Do not open or service any power supply assembly.**
- **Do not connect or disconnect any cables or perform installation, maintenance, or reconfiguration of this product during an electrical storm.**
- **The product might be equipped with multiple power cords. To remove all hazardous voltages, disconnect all power cords.**
- **Connect all power cords to a properly wired and grounded electrical outlet. Ensure that the outlet supplies proper voltage and phase rotation according to the system rating plate.**
- **Connect any equipment that will be attached to this product to properly wired outlets.**
- **When possible, use one hand only to connect or disconnect signal cables.**
- **Never turn on any equipment when there is evidence of fire, water, or structural damage.**
- **Disconnect the attached power cords, telecommunications systems, networks, and modems before you open the device covers, unless instructed otherwise in the installation and configuration procedures.**
- **Connect and disconnect cables as described in the following procedures when installing, moving, or opening covers on this product or attached devices.**

  To disconnect:
  a. **Turn off everything (unless instructed otherwise).**
  b. **Remove the power cords from the outlets.**
  c. **Remove the signal cables from the connectors.**
  d. **Remove all cables from the devices.**

  To connect:
  a. **Turn off everything (unless instructed otherwise).**
  b. **Attach all cables to the devices.**
  c. **Attach the signal cables to the connectors.**
  d. **Attach the power cords to the outlets.**
  e. **Turn on the devices.**
- **Sharp edges, corners and joints may be present in and around the system. Use care when handling equipment to avoid cuts, scrapes and pinching.**

(D005)

4. Remove the cryptographic coprocessor from the PCIe bus slot in the host computer.

   Attention: Electrostatic discharge (ESD) can damage the card and its components. Wear an ESD wrist-strap while handling and installing the card, or take the following precautions:

   - Limit your movements; this helps prevent static electricity building up around you.
   - Prevent others from touching the card or other components.
   - Handle the card by its edges only. Do not touch exposed circuitry and components.

5. Insert one of the new batteries into the battery tray. Align the “+” on the battery with the “+” on the battery tray (the end with the red wire). Connect the tray’s wires to the J2302 connector; see Figure 1 on page 6. The connector is polarized to ensure a proper connection.

   Note: The J2302 connector has three pins. The top pin is the "-" pin, while the bottom pin (marked with a white dot next to it) is the "+" pin.

   Attention: Any loss of power erases data stored in the card’s protected memory. To prevent loss, ensure that the battery tray contains a fresh battery and is attached to the J2302 connector.

6. Remove the battery attention labels from the battery holders on the card. These labels can be torn off and discarded. They are to be replaced by the spare labels included with the replacement batteries.
7. Remove the battery from the BT1 position of the coprocessor. To eject the battery, turn the coprocessor over and insert a small object, such as a screwdriver, through the hole to eject the battery.
8. Replace the battery in the BT1 position with a new battery, aligning the polarities as marked.
9. Replace the battery in the BT2 position with the battery in the battery tray, aligning the polarities as marked. (The new battery already installed in the BT1 position provides sufficient power to the coprocessor while you perform this step.)
10. Unplug the battery tray from the J2302 connector.
11. Apply the replacement battery-attention labels onto the holders on the card.
12. Reinsert the coprocessor into the PCIe bus slot, with no cards installed in any adjacent slots. Be sure that the card is fully seated. Replace the bracket-holding screw as needed.
13. Replace the host computer's cover.
14. Reconnect any power cables, and any other cables that were previously disconnected.
15. Turn the computer ON. The coprocessor runs its power-on self-test (POST).
16. The batteries are lithium 3.0 volt batteries. Recycle or dispose of the old batteries as required by local law. See "Battery return program" on page xii.

You have completed the procedure for replacing the PCIe cryptographic coprocessor batteries.

Chapter 4. Guidelines for transporting a coprocessor

This section provides guidelines to follow when it becomes necessary to travel with or ship an IBM 4765 PCIe Cryptographic Coprocessor. This chapter addresses protecting the coprocessor from physical damage. It also touches on some export and import considerations. This chapter does not attempt to address issues with data security.

The guidelines provided below are meant to assist you in properly transporting your coprocessor. Following these guidelines does not guarantee that your coprocessor or the data that it contains will arrive unharmed. You are ultimately responsible for taking whatever measures are necessary to adequately protect your coprocessor and its data. At a minimum, the coprocessor must be maintained within the environmental specifications shown in Table 1 on page 3.

Note: There is no X-ray tamper sensor on the coprocessor.

Handling the coprocessor

Electrostatic discharge (ESD) can damage the coprocessor and its components. Wear an ESD wrist-strap while handling the coprocessor, or take the following precautions:

- Limit your movements; this helps prevent static electricity from building up around you.
- Prevent others from touching the card or other components.
- Before removing the coprocessor from the ESD barrier bag, touch the bag to an unpainted metal surface on your computer and hold it there for at least two seconds.

Handle the coprocessor by its edges only. Do not touch exposed circuitry and components.

International transport

International transport of a cryptographic coprocessor requires special consideration of applicable export laws, regulations, and controls. For example, the export of a cryptographic coprocessor to certain countries might be restricted. When hand carrying a coprocessor, consider taking with you proof-of-purchase documents to protect against duty assessment. When shipping a coprocessor, there may be a Customs declaration form that must be completed. Any existing company policies should be considered as well.

Traveling with a coprocessor

Whenever traveling with a coprocessor, keep it in the ESD barrier bag that the coprocessor was shipped in, or a bag with similar properties. Ensure that the bag has not been damaged and is in good condition.

Use enough cushioning and packing materials as deemed necessary to protect the coprocessor. Consider these forces, expected or otherwise:

- Vibration
- A hard knock or blow
- A crushing load
- Bending or flexing
- A piercing object

If the coprocessor could be subject to extreme hot or cold temperatures, such as when it is in the cargo hold of an airplane or left in a parked vehicle, it is recommended that it be packed as if you were shipping a coprocessor. See “Shipping a coprocessor” on page 14.

Shipping a coprocessor

When shipping a coprocessor, it is recommended that it be shipped using the original package materials. See Figure 2. These materials include the following:

- A cardboard box
- Six firm pieces of white polystyrene foam (two large pieces, two long pieces, and two short pieces)
- Six soft pieces of foam (two egg-crate pieces with a rectangular hole in the center, two long and thin pieces, and two short and thick pieces)
- Two large bags, each containing an isothermal gel
- One small bag, containing a desiccant of hard granules or beads of silica gel
- One ESD barrier bag

Figure 2. IBM 4765 PCIe Cryptographic Coprocessor packaging material

Using the above materials, follow these steps to repack the coprocessor:

1. Cover the bottom of the cardboard box with one of the two large pieces of firm foam.
2. Fill the perimeter of the box with the two long pieces and two short pieces of firm foam. Face the narrow side down.
3. Place a long and thin piece of soft foam parallel to each of the two short pieces of firm foam. Face the narrow side down.
4. Place a short and thick piece of soft foam parallel to and centered with each of the two long pieces of firm foam. Face the narrow side down.

5. Reposition the long and thin pieces of soft foam against the short and thick pieces of soft foam. This makes a rectangle which should be centered in the box.
6. Place an isothermal bag, which has been kept at room temperature (not frozen), in each of the two narrow spaces left by the rectangle.
7. Tuck each bag so that it does not protrude above the foam.
8. Place the small bag of desiccant inside the rectangle.
9. Cover the bottom of the rectangle with one of the egg-crate pieces of foam. Face the smooth side down.
10. Place the coprocessor in the ESD barrier bag. Use proper handling procedures as described above.
11. Fold the open end of the bag over and tape closed.
12. Place the sealed bag in the rectangle, on top of the egg-crate foam.
13. Cover the sealed bag with the remaining egg-crate foam. Face the smooth side up.
14. Cover the contents of the cardboard box with the remaining large piece of firm foam.
15. Place contact and destination information inside the box.
16. Fold over the two small flaps of the cardboard box, followed by the two large flaps, and securely tape closed.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you. Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at: www.ibm.com/legal/copytrade.shtml

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries

Electronic emissions

Federal Communications Commission (FCC) statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult an IBM-authorized dealer or service representative for help.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. Proper cables and connectors are available from IBM authorized dealers. IBM is not responsible for any radio or television interference caused by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Industry Canada Compliance Statement

This Class B digital apparatus complies with Canadian ICES-003.

Avis de conformité à la réglementation d'Industrie Canada

Cet appareeil numérique de la classe B respecte est conforme à la norme NMB-003 du Canada.

European Community Compliance Statement

This product is in conformity with the protection requirements of EU Council Directive 2004/108/EC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM® cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the fitting of non-IBM option cards.

This product has been tested and found to comply with the limits for Class B Information Technology Equipment according to European Standard EN 55022. The limits for Class B equipment were derived for typical residential environments to provide reasonable protection against interference with licensed communication equipment.

European Community contact:
IBM Deutschland GmbH
Technical Regulations, Department M456
IBM-Allee 1, 71139 Ehningen, Germany
Telephone: +49 7032 15-2937
E-mail: tjahn@de.ibm.com

Deutschsprachiger EU Hinweis:

Hinweis fur Gerate der Klasse B EU-Richtlinie zur Elektromagnetischen Vertraglichkeit

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie2004/108/EG zur Angleichung der Rechtsvorschriften uber die elektromagnetischeVertraglichkeit in den EU-Mitgliedsstaatenund halt die Grenzwerte der EN 55022 Klasse B ein. Um dieses sicherzustellen, sind die Gerate wie in den Handbuchern beschrieben zu installieren und zu betreiben. Des Weiteren durfen auch nur von der IBM empfohlene Kabelangeschlossen werden.IBM ubernimmt keine Verantwortung fur die Einhaltung der Schutzanforderungen, wenn dasProdukt ohne Zustimmung von IBM verandert bzw. wenn Erweiterungskomponenten vonFremdherstellern ohne Empfehlung von IBM gesteckt/eingebaut werden.

Deutschland: Einhaltung des Gesetzes uber die elektromagnetische Vertraglichkeit von Geraten

Dieses Produkt entspricht dem “Gesetz uber die elektromagnetische Vertraglichkeit vonGeraten (EMVG)“. Dies ist die Umsetzung der EU-Richtlinie 2004/108/EG in derBundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz uber die elektromagnetische Vertraglichkeit von Geräten (EMVG) (bzw. der EMC EG Richtlinie 2004/108/EG) fur Gerate der Klasse B

Dieses Gerat ist berechtigt, in Ubereinstimmung mit dem Deutschen EMVG das EG-Konformitatszeichen - CE - zu fuhren.

Verantwortlich fur die Einhaltung der EMV-Vorschriften ist der Hersteller: International Business Machines Corp. New Orchard Road Armonk, New York 10504 Tel: 914-499-1900

Der verantwortliche Ansprechpartner des Herstellers in der EU ist: IBM Deutschland GmbH Technical Regulations, Abteilung M456IBM-Allee 1, 71139 Ehningen, Germany Tel: +49 7032 15-2937 e-mail: tjahn@de.ibm.com

Generelle Informationen:

Das Gerat erfullt die Schutzanforderungen nach EN 55024 und EN 55022 Klasse B.

VCCI Statement - Japan

この装置は、クラスB情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。

取扱説明書に従って正しい取り扱いをして下さい。

VCCI－B

IBM Taiwan Contact Information:

台灣IBM 產品服務聯絡方式：
台灣國際商業機器股份有限公司
台北市松仁路7號3樓
電話：0800-016-888

Electromagnetic Interference (EMI) Statement - Korea

이 기기는 가정용(B급)으로 전자파적합기기로서 주로 가정에서 사용하는 것을 목적으로 하며, 모든 지역에서 사용할 수 있습니다.

Glossary

This glossary includes some terms and definitions from the *IBM Dictionary of Computing*, New York: McGraw Hill, 1994. This glossary also includes some terms and definitions from:

- The *American National Standard Dictionary for Information Systems*, ANSI X3.172-1990, copyright 1990 by the American National Standards Institute (ANSI). Copies may be purchased from the American National Standards Institute, 11 West 42 Street, New York, New York 10036. Definitions are identified by the symbol (A) following the definition.
- The *Information Technology Vocabulary*, developed by Subcommittee 1, Joint Technical Committee 1, of the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC JTC1/SC1). Definitions of published parts of this vocabulary are identified by the symbol (I) following the definition; definitions taken from draft international standards, committee drafts, and working papers being developed by ISO/IEC JTC1/SC1 are identified by the symbol (T) after the definition, indicating that final agreement has not yet been reached among the participating National Bodies of SC1.

A

American National Standards Institute (ANSI). An organization consisting of producers, consumers, and general interest groups that establishes the procedures by which accredited organizations create and maintain voluntary industry standards in the United States. (A)

B

bus. In a processor, a physical facility along which data is transferred.

C

card. An electronic circuit board that is plugged into a slot in a system unit. A plug-in circuit assembly.

coprocessor. A supplementary processor that performs operations in conjunction with another processor. A microprocessor on an expansion card that extends the address range of the processor in the host system or adds specialized instructions to handle a particular category of operations; for example, an I/O coprocessor, math coprocessor, or networking coprocessor.

cryptography. The transformation of data to conceal its meaning. In computer security, the principles, means and methods used to so transform data.

E

EEPROM. See *electrically erasable programmable read-only memory*.

electrostatic discharge (ESD). An undesirable discharge of static electricity that can damage equipment and degrade electrical circuitry.

electrically erasable programmable read-only memory (EEPROM). A type of memory chip that can retain its contents without consistent electrical power. Unlike the PROM, which can be programmed only once, the EEPROM can be erased electrically. Because it can only be reprogrammed a limited number of times before it wears out, it is appropriate for storing small amounts of data that are changed infrequently.

expansion card. A circuit board that a user can install in an expansion slot to add memory or special features to a computer. Synonym for *card*.

expansion slot. One of several receptacles available inside a computer, into which a user can install an expansion card.

F

feature. Part of an IBM product able to be ordered separately.

Federal Communications Commission (FCC). A board of commissioners, appointed by the President under the Communications Act of 1934, having the power to regulate all interstate and foreign communications in the United States that are transmitted by wire or radio.

Federal Information Processing Standard (FIPS). A standard published by the US National Institute of Science and Technology.

FIPS. See *Federal Information Processing Standard*.

I

interface. A shared boundary between two functional units, defined by functional characteristics, signal characteristics, or other characteristics, as appropriate. The concept includes the specification of the connection of two devices having different functions. (T) Hardware, software, or both, that links systems, programs, and devices.

International Organization for Standardization (ISO). An organization of national standards bodies established to promote the development of standards to facilitate the international exchange of goods and services, and to develop cooperation in intellectual, scientific, technological, and economic activity.

J

jumper. A wire that joins two unconnected circuits.

K

key. In computer security, a sequence of symbols used with an algorithm to encipher or decipher data.

P

power-on self-test (POST). A series of diagnostic tests that are run automatically by a device when the power is turned on.

S

security. For computers, the protection of data, system operations, and devices from accidental or intentional ruin, damage, or exposure.

Numerics

4765. IBM 4765 PCIe Cryptographic Coprocessor.

Index

B

battery
  disposal 11
  replacement 9
  tray 9, 10
battery removal warning 2
battery return xii
battery-powered protected memory 1, 9

C

card return xiii
caution notices, coprocessor 5, 9
CCA cryptographic coprocessor support program 2
certified device key, coprocessor 1
contents
  battery-replacement kit 9
  coprocessor package 1
coprocessor
  See PCIe cryptographic coprocessor

D

device key, certified 1
dimensions, coprocessor 3

E

electronic emissions 18
electrostatic discharge (ESD) 6, 10
environmental notices xi

H

handling considerations, coprocessor 1
hardware requirements, coprocessor 2
humidity
  See operating environment

I

installing coprocessor 5

J

jumper settings 7

K

kit contents, battery replacement 9

L

label
  slot cover 1

M

memory
  See battery-powered protected memory
module, tamper-resistant 1

N

notices
  notices statement 17

O

operating environment
  environmental specifications 2
  power requirements 2

P

package contents 1
packing guidelines 13
PCIe cryptographic coprocessor
  caution notices 5, 9
  contents 1
  device key, certified 1
  dimensions 3
  environmental specification 2
  handling considerations 1
  hardware requirements 2
  installation 5
  introduction 1
  power requirements 2
  process objects 1
  shipping 1
  software 2
  specifications 2
  storage 1
  storage requirements 2
  support program 2
  tamper sensors 1
  temperature 2
  travel guidelines 13
power-on self-test (POST) 7, 11
power, coprocessor
  See also operating environment
  active mode 2
  voltage 2
process objects, coprocessor
  bulk data 1
  certificates 1
  cryptographic keys 1
product recycling and disposal xi
product return xiii
protected memory
  See battery-powered protected memory

R

recycling and disposal xi
replacing batteries 9

S

safety notices ix
shipping, coprocessor 1
slot cover label 1
software, coprocessor 2
specifications, coprocessor
  environmental specifications 2
  hardware 2
  physical dimensions 3
  power requirements 2
  software 2
storage, coprocessor 1, 2
support program, CCA cryptographic coprocessor 2

T

tamper sensors, coprocessor 1
tamper-resistant module 1
temperature, coprocessor
  See also operating environment
  shipping 2
  storage 2
traveling with coprocessor 13

W

world trade safety x

X

X-ray tamper 13